ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

# **Cyber Intelligence:** Digital Footprint Collection on the Internet **(OSINT)**

## KEY FIGURES

- **83% of SMEs** are **not prepared** to respond to a cyber attack.
- **30% of SMEs** fear **phishing** as one of their main cyber threats.
- **91% of SMEs** still do **not** have **cyber liability insurance.**

## OVERVIEW

SMEs face a series of complex challenges, spurred by a tremendously agile and constantly evolving market. From economic uncertainty to fierce competition, SMEs must adapt to changing trends and the rapid evolution of technology, staying updated and flexible to ensure the relevance of their products and services. Digitalization is also highlighting the growth of the attack surface, thereby increasing the likelihood of experiencing a cyber incident and the potential consequences it can have for their survival.

## SOLUTIONS

We deeply understand the needs of SMEs and strive to fulfill them by designing, implementing, maintaining, and operating comprehensive security plans based on the six functions of NIST (Governance, Identification, Protection, Detection, Response, and Recovery). Among these, our Digital Footprint Collection service (OSINT) allows for the discovery of various data exposed on the Internet (including the Deep and Dark Web) of your organization, including its Shadow IT. With this information, you can anticipate potential attacks, close gaps, and adequately protect your information.

Within the **external Shadow IT** of your organization, we can identify, among others, the following exposed assets:

- Websites launched within marketing campaigns on external hosting.
- Sites published through vendors, without IT control.
- Applications and other services contracted to external companies.
- Testing environments (development, quality, or pre-production) published on the Internet.
- APIs with access to internal information.
- Domains and subdomains registered but unused.
- Cloud environments without IT control.
- Corporate environments with uncontrolled data (Google Drive, AWS…).
- IP addresses without associated domains.
- Websites inventoried embedded in third-party iFrames.

Additionally, among the **data exfiltrated on the Internet** of your organization, we can identify the following:

- Credentials.
- Phones.
- Addresses.
- Usernames.
- Social networks.
- Secrets.
- Patents.
- Bins & Credit cards.

**ABOUT ZEROLYNX**

European Cybersecurity and Intelligence Provider.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY™ MADE IN EUROPE